

AMENDMENTS TO THE CLAIMS

1. (Currently amended) A security communication packet processing apparatus that performs at least one of encryption processing, decryption processing and authentication processing to ~~a~~ an inputted packet, said security communication packet processing apparatus comprising:

~~one or more~~ at least one encryption processing unit operable to perform the encryption processing and the decryption processing in a data block unit of B1 bits;

~~one or more~~ at least one authentication processing unit operable to perform the authentication processing in a data block unit of B2 ($= n \times B1$) bits in parallel to the encryption processing or the decryption processing performed by ~~the~~ said at least one encryption processing unit, and output an authentication value indicating the result of the authentication processing, the data block unit of B2 bits being n times the data block unit of B1 bits;

~~one or more~~ at least one data block accumulation unit operable to accumulate the data blocks to which the encryption processing ~~is~~ has been performed by ~~the~~ said at least one encryption processing unit, and, when the amount of accumulated amount of the data blocks reaches B2 bits, output the data blocks to ~~the~~ said at least one authentication processing unit;

a packet construction unit operable to receive the encrypted or decrypted data blocks from ~~the~~ said one or more encryption processing ~~unit~~ units, receive the authentication value from ~~the~~ said one or more authentication processing ~~unit~~ units, and construct a packet including the received data blocks and the authentication value; and

a control unit operable to divide the inputted packet into the data blocks of B1 bits, and output the data blocks sequentially to ~~the~~ said at least one encryption processing unit.

2. (Currently Amended) The security communication packet processing apparatus according to Claim 1, wherein:

~~wherein the~~ said control unit judges is operable to judge whether ~~which type~~ the inputted packet is, ~~the~~ a first type packet requiring the encryption processing and the authentication processing, the a second type packet requiring the decryption processing

and the authentication processing, ~~the~~ a third type packet requiring one of the encryption processing and the decryption processing, or ~~the~~ a fourth type packet requiring the authentication processing only;

when said control unit judges that the inputted packet is judged to be the first type packet, ~~divides~~ said control unit is operable to divide the packet into the data blocks of B1 bits and ~~outputs~~ output the data blocks sequentially to ~~the~~ said at least one encryption processing unit;

when said control unit judges that the inputted packet is judged to be the second type packet, ~~divides~~ said control unit is operable to divide the packet into the data blocks of B1 bits, ~~outputs them~~ output the data blocks of B1 bits sequentially to ~~the~~ said encryption processing unit, ~~divides~~ divide the packet or ~~the~~ a duplicate of the packet into the data blocks of B2 bits, and ~~outputs~~ output the data blocks of B2 bits sequentially to ~~the~~ said at least one authentication processing unit;

when said control unit judges that the inputted packet is judged to be the third type packet, ~~divides~~ said control unit is operable to divide the packet into the data blocks of B1 bits and ~~outputs~~ output the data blocks sequentially to ~~the~~ said at least one encryption processing unit; and

when said control unit judges that the inputted packet is judged to be the fourth type packet, ~~divides~~ said control unit is operable to divide the packet into the data blocks of B2 bits and ~~outputs~~ output the data blocks sequentially to ~~the~~ said at least one authentication processing unit.

3. (Currently Amended) The security communication packet processing unit according to Claim 1, wherein:

~~wherein~~ the number of at least one of ~~the~~ said at least one encryption processing unit and ~~the~~ said at least one authentication processing unit is two or more; and

the number of ~~the~~ said at least one data block accumulation unit is equal to ~~that~~ the number of the said at least one encryption processing unit.

4. (Currently Amended) The security communication packet processing apparatus according to Claim 3, wherein ~~the~~ said control unit specifies is operable to specify, among

two or more encryption processing units or two or more authentication processing units, ~~the said~~ encryption processing unit or ~~the said~~ authentication processing unit that is ready for processing, and ~~outputs-output~~ the data blocks to the specified encryption processing unit or ~~the~~ authentication processing unit.

5. (Currently Amended) The security communication packet processing apparatus according to Claim 1, further comprising: a data path connection switching unit that ~~can~~operable to connect the output of ~~the said~~ control unit and the input of ~~the said~~ at least one encryption processing unit, the output of ~~the said~~ control unit and the input of ~~the said~~ at least one authentication processing unit, the output of ~~the said~~ at least one encryption processing unit and the input of ~~the said~~ at least one data block accumulation unit, and the output of ~~the said~~ at least one data block accumulation unit and the input of ~~the said~~ at least one authentication processing unit, respectively and independently.

6. (Currently Amended) The security communication packet processing apparatus according to Claim 5, wherein:

~~wherein the said~~ control unit ~~judges-is operable to judge whether~~ which type the inputted packet is, ~~the~~ a first type packet requiring the encryption processing and the authentication processing, ~~the~~ a second type packet requiring the decryption processing and the authentication processing, ~~the~~ a third type packet requiring one of the encryption processing and the decryption processing, or ~~the~~ a fourth type packet requiring the authentication processing only;

when said control unit judges that the inputted packet is judged to be the first type packet, ~~controls-said control unit is operable to control said~~ the data path connection switching unit so as to connect the output of the said control unit and the input of the said at least one encryption processing unit, the output of the said at least one encryption processing unit and the input of the said at least one data block accumulation unit, and the output of the said at least one data block accumulation unit and the input of the said authentication processing unit;

when said control unit judges that the inputted packet is judged to be the second type packet, ~~controls-said control unit is operable to control said~~ the data path connection

switching unit so as to connect the output of ~~the said~~ control unit and the input of ~~the said~~ at least one encryption processing unit, and the output of ~~the said~~ control unit and the input of ~~the said~~ at least one authentication processing unit;

when ~~said control unit judges that the inputted packet is judged to be the third type packet, controls~~ said control unit is operable to control said the data path connection switching unit so as to connect the output of ~~the said~~ control unit and the input of ~~the said~~ at least one encryption processing unit; and

when ~~said control unit judges that the inputted packet is judged to be the fourth type packet, controls~~ said control unit is operable to control said the data path connection switching unit so as to connect the output of ~~the said~~ control unit and the input of ~~the said~~ at least one authentication processing unit.

7. (Currently Amended) The security communication packet processing apparatus according to Claim 6, wherein:

~~wherein~~ the number of at least one of ~~the said~~ at least one encryption processing unit and ~~the said~~ at least one authentication processing unit is two or more; and

the number of ~~the said~~ at least one data block accumulation unit is equal to ~~that~~ the number of the said at least one encryption processing unit.

8. (Currently Amended) The security communication packet processing apparatus according to Claim 7, wherein ~~the said~~ control unit ~~specifies~~ is operable to specify, among two or more encryption processing units or two or more authentication processing units, ~~the said~~ encryption processing unit or ~~the said~~ authentication processing unit that is ready for processing, and ~~makes~~ make ~~said~~ the data path connection switching unit perform a connection for the specified encryption processing unit or ~~the~~ authentication processing unit.

9. (Currently amended) The security communication packet processing apparatus according to Claim 1, further comprising: a processing data saving unit; provided for each of at least one of ~~the said~~ at least one encryption processing unit, ~~the said~~ at least one authentication processing unit and ~~the said~~ at least one data block accumulation unit,

~~that has~~each processing data saving unit having a memory area for temporarily suspending the processing of the data blocks in the processing unit for which said processing data saving unit is provided, and saving the data blocks which ~~are~~ were being processed in the processing unit corresponding respectively to the processing unit.

10. (Currently amended) The security communication packet processing apparatus according to Claim 9, wherein ~~the said~~ control unit ~~specifies~~is operable to specify the processing unit that is performing the processing of the data blocks of the packet with the lowest priority among the processing units, and, after suspending the processing of the data blocks in the processing unit and saving the data blocks which ~~are~~ were being processed in the processing unit into ~~the said~~ processing data saving unit provided to the processing unit performing the processing of the data blocks of the packet with the lowest priority, ~~makes~~ make the processing unit perform the processing of the data blocks of the inputted packet.

11. (Currently Amended) The security communication packet processing apparatus according to Claim 10, further comprising: ~~the~~ a data path connection switching unit ~~that can~~operable to connect the output of ~~the said~~ control unit and the input of ~~the said~~ at least one encryption processing unit, the output of ~~the said~~ control unit and the input of ~~the said~~ at least one authentication processing unit, the output of ~~the said~~ at least one encryption processing unit and the input of ~~the said~~ at least one data block accumulation unit, and the output of ~~the said~~ at least one data block accumulation unit and the input of ~~the said~~ at least one authentication processing unit, respectively and independently.

12. (Currently Amended) The security communication packet processing apparatus according to Claim 11, wherein:

~~wherein~~ the number of at least one of the said at least one encryption processing unit and ~~the said~~ at least one authentication processing unit is two or more; and

the number of ~~the said~~ at least one data block accumulation unit is equal to ~~that~~ the number of the said at least one encryption processing unit.

13. (Currently amended) The security communication packet processing apparatus according to Claim 1, further comprising: ~~the~~ a processing data saving unit; provided for each of at least two of ~~the~~ said at least one encryption processing unit, ~~the~~ said at least one authentication processing unit and ~~the~~ said at least one data block accumulation unit, ~~that has each processing data saving unit having~~ a memory area shared by the processing units for temporarily suspending the processing of the data blocks in the processing unit and saving the data blocks which are-were being processed in the processing units.

14. (Currently amended) The security communication packet processing apparatus according to Claim 13, wherein ~~the~~ said control unit ~~specifies~~ is operable to specify, among the processing units, the processing unit that is performing the processing of the data blocks of the packet with the lowest priority, and, after suspending the processing of the data blocks in the processing unit and saving the data blocks which ~~are-were~~ being processed in the processing unit in ~~the~~ said processing data saving unit provided to the processing unit performing the processing of the data blocks of the packet with the lowest priority, makes-make the processing unit perform the processing of the data blocks of the inputted packet.

15. (Currently Amended) The security communication packet processing apparatus according to Claim 14, further comprising: ~~the~~ a data path connection switching unit ~~that can~~ operable to connect the output of ~~the~~ said control unit and the input of ~~the~~ said at least one encryption processing unit, the output of ~~the~~ said control unit and the input of ~~the~~ said at least one authentication processing unit, the output of ~~the~~ said at least one encryption processing unit and the input of ~~the~~ said at least one data block accumulation unit, and the output of ~~the~~ said at least one data block accumulation unit and the input of ~~the~~ said at least one authentication processing unit, respectively and independently.

16. (Currently Amended) The security communication packet processing apparatus according to Claim 15, wherein:

~~wherein~~ the number of at least one of ~~the~~ said at least one encryption processing unit and ~~the~~ said at least one authentication processing unit is two or more; and

the number of ~~the said~~ at least one data block accumulation unit is equal to that ~~the number of the said~~ at least one encryption processing unit.

17. (Previously Presented) The security communication packet processing apparatus according to Claim 1, wherein the B1 is 64, and the B2 is 512.

18. (Currently Amended) A security communication packet processing method that performs at least one of the encryption processing, decryption processing and the authentication processing to the an inputted packet, said security communication packet processing method comprising including:

~~a dividing step for dividing the inputted packet into the data blocks of B1 bits;~~

~~an encryption processing step for performing the encryption processing or the decryption processing to the divided data blocks of B1 bits;~~

~~a data block accumulating step for accumulating the encrypted data blocks and outputting the data blocks when the amount of accumulated amount of the data blocks reaches B2 (=n×B1)-bits, B2 bits being n times the number of B1 bits;~~

~~an authentication processing step for performing the authentication processing to the outputted data blocks of B2 bits in parallel to the encryption processing or the decryption processing, and outputting the authentication value indicating the result of the authentication processing;~~

~~a packet constructing step for receiving the encrypted or decrypted data blocks, receiving the outputted authentication value, and constructing the packet including the received data blocks and the authentication value.~~

19. (Currently Amended) The security communication packet processing method according to Claim 18, further including comprising:

~~a control step for judging whether which type the inputted packet is, the a first type packet requiring the encryption processing and the authentication processing, the a second type packet requiring the decryption processing and the authentication processing, the a third type packet requiring only one of the encryption processing and the decryption processing, or the a fourth type packet requiring the authentication processing only, and~~

when ~~it~~ the inputted packet is judged to be the first type packet, controlling so that the division in ~~the dividing steps~~ said dividing of the inputted packet, the encryption processing ~~in the performed in said performing of the encryption processing step or the decryption processing~~, the accumulation in ~~the data block~~ said accumulating step of the encrypted data blocks, the authentication processing ~~performed in the said performing of the authentication processing step~~ and the construction ~~performed in the said constructing of the packet constructing step~~ are performed.

20. (New) The security communication packet processing apparatus according to claim 5, wherein said data path connection switching unit is operable to switch a data path between two of said control unit, said at least one encryption processing unit, said at least one authentication processing unit and said at least one data block accumulation unit, so that only packets A pass through said at least one data block accumulation unit and only packets B bypass said at least one data block accumulation unit, the packets A being a packet which requires both encryption processing and authentication processing and a packet which requires both decryption processing and authentication processing, and the packets B being a packet which requires only encryption processing, a packet which requires only decryption processing and a packet which requires only authentication processing.

21. (New) The security communication packet processing apparatus according to claim 9, wherein the data blocks are saved from said at least one encryption processing unit and said at least one authentication processing unit into said processing data saving unit, and the saved data blocks are restored from said processing data saving unit to the said at least one encryption processing unit and said at least one authentication processing unit, via said at least one data block accumulation unit.

22. (New) The security communication packet processing apparatus according to claim 14, wherein said control unit is further operable to make another processing unit read the data blocks from said processing data saving unit and restart the processing, the another processing unit having a function equivalent to a function of the processing unit

performing the processing of the data blocks of the packet with the lowest priority, from which processing unit the data blocks are saved into said processing data saving unit.